CLAIMS

Thus, having described the systems and methods for virus checking software code, we claim the following:

1. A method for identifying infected program instructions, comprising the steps of:

inserting a dynamic execution layer interface (DELI) between computing device hardware and the program instructions;

monitoring the program instructions as they enter the DELI to determine if the code has been previously processed by the computing device hardware; and when it is the case that the application code has not been previously processed,

analyzing the program instructions to determine if program instructions are infected.

2. The method of claim 1, wherein the step of analyzing the program instructions comprises an investigation of the contents of instructions within code fragments.

3. The method of claim 1, wherein the step of analyzing the program instructions comprises inserting decrypted program instructions into a virus detection manager.

4. The method of claim 3, further comprising the step of:

releasing program instructions from the virus detection manager when infected program instructions are not detected.

5. The method of claim 3, wherein the step of analyzing the program instructions comprises performing a signature comparison with the contents of the code fragments.

6. The method of claim 3, wherein the step of analyzing the program instructions comprises monitoring the behavior of the contents of the code fragments in a virtual computing device.

7. The method of claim 3, wherein the step of analyzing the program instructions comprises applying a plurality of tests on the contents of the code fragments in a virtual computing device.

8. The method of claim 4, further comprising the step of:
processing the released program instructions in computer hardware.

9. A system for detecting infected program instructions in active software applications, comprising:
means for intercepting program instructions;
means for determining when the intercepted program instructions have not been processed by the computing device; and
means for analyzing the intercepted program instructions that have not been processed by the computing device prior to forwarding the intercepted program instructions to computer hardware.

10. The system of claim 9, further comprising:
means for gaining control over execution of program instructions.

11. The system of claim 9, further comprising:
means for executing program instructions.

12. The system of claim 9, wherein the means for intercepting comprises a dynamic execution layer interface (DELI).

13. The system of claim 9, wherein the means for analyzing the intercepted program instructions comprises a virus detection manager.

14. The system of claim 13, wherein the virus detection manager comprises a controller configured to apply a plurality of virus detection tests over the contents of the intercepted program instructions.

15. A virus detection program stored on a computer-readable medium, comprising:

logic configured to intercept program instructions;

logic configured to determine if the intercepted program instructions have not been processed by a computing device; and

logic configured to determine when the intercepted program instructions that have not been processed by the computing device are infected with a virus.

16. The program of claim 15, further comprising:

logic configured to gain control over execution of intercepted program instructions.

17. The program of claim 15, further comprising:

logic configured to execute program instructions.

18. The program of claim 15, further comprising:

logic configured to forward non-infected intercepted program instructions to the computing device.

19. A computer system, comprising:

a processor;

an execution memory;

a dynamic execution layer interface (DELI) residing between at least one application and the processor, wherein the DELI comprises:

a core configured to cache and execute certain application code fragments;

an application programming interface configured to provide access to caching and executing functions of the core to a virus detection manager; and

a system control and configuration layer configured to provide policies for operation of the core.

20. The system of claim 19, wherein the virus detection manager is configured to apply at least one virus detection test on the contents of application code fragments.

21. The system of claim 19, wherein the core is configured to process executable application code fragments from the at least one application that have not been previously sent to the processor.

22. The system of claim 21, wherein the virus detection manager controls whether application code fragments are released to the processor.

23. The system of claim 22, wherein application code fragments that contain at least one virus signature are not released to the processor.

24. The system of claim 22, wherein application code fragments that behave in a manner consistent with known virus attacks are not released to the processor.